Programmazione in Rete

a.a. 2005/2006

http://www.di.uniba.it/~lisi/courses/prog-rete/prog-rete0506.htm

dott.ssa Francesca A. Lisi
lisi@di.uniba.it

Orario di ricevimento: mercoledì ore 10-12

dib

Sommario della lezione di oggi: La sicurezza nelle reti (1/3)

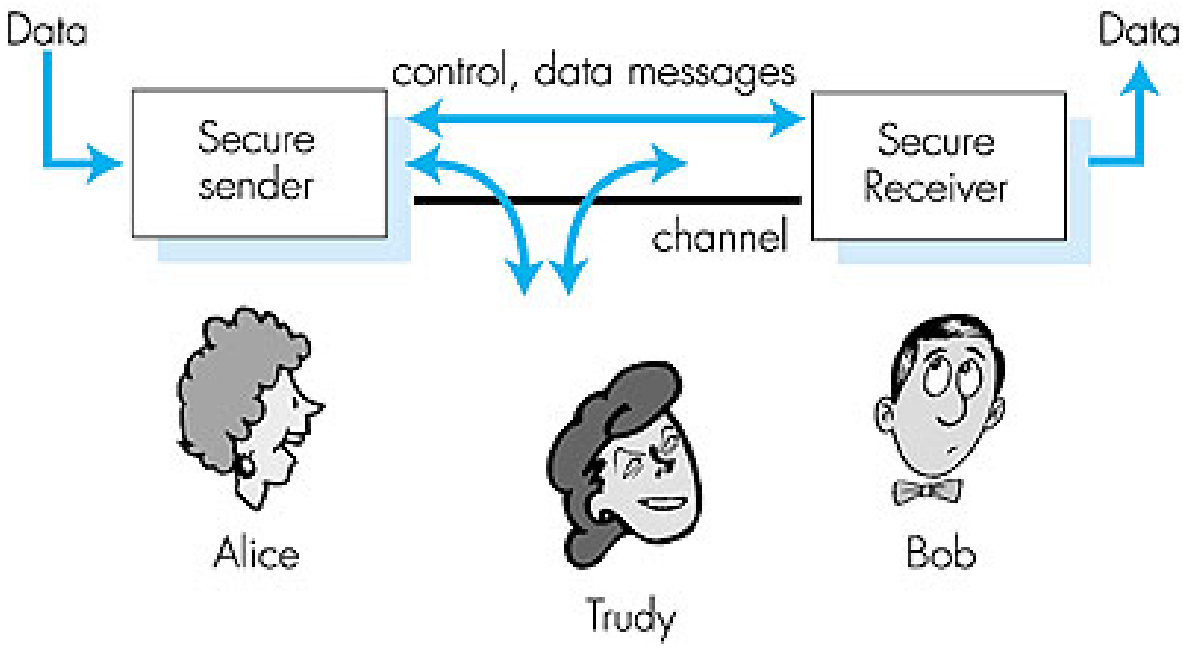
Dai fondamenti ...

- che cosa è la sicurezza?
- crittografia
- autenticazione
- integrità e non ripudiabilità del messaggio
- distribuzione delle chiavi e certificazione

... in pratica

- a livello di applicazione: e-mail sicura
- a livello di trasporto: commercio Internet, SSL, SET
- a livello di rete: sicurezza IP

Amici e nemici: Alice, Bob, Trudy



- Bob e Alice (amanti!) vogliono comunicare "in modo sicuro"
- Trudy (l'intrusa) potrebbe intercettare, cancellare, aggiungere messaggi

Cos'è la sicurezza delle reti?

Segretezza: solo il mittente e il destinatario inteso dovrebbero "comprendere" il contenuto di un messaggio

- il mittente cripta il messaggio
- il destinatorio decripta il messaggio

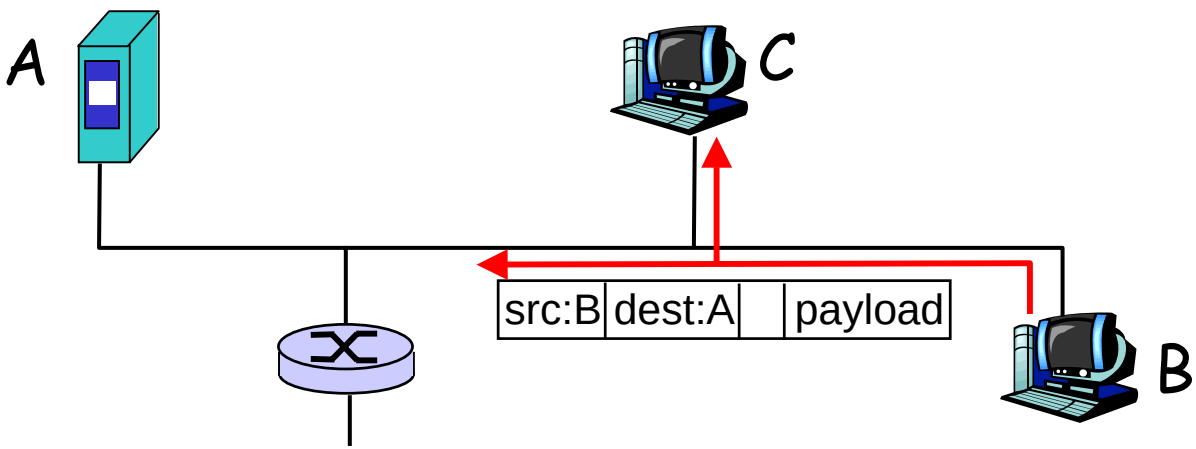
Autenticazione: mittente e destinatario vogliono conferme su identità reciproca

Integrità del messaggio: mittente e destinatorio vogliono assicurare che il messaggio sia inalterato (in transito, o in seguito)

Minacce alla sicurezza di Internet

Packet sniffing:

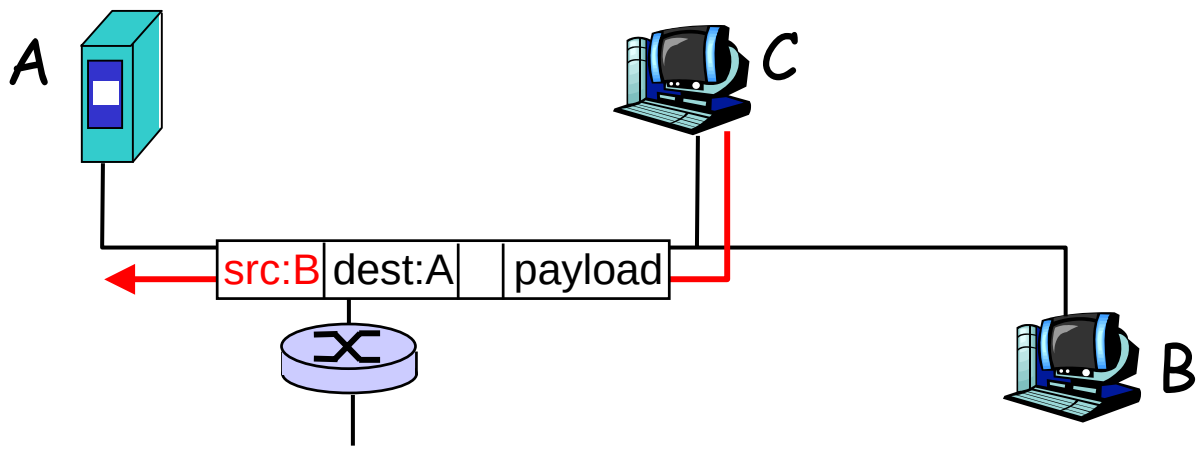
- broadcast media
- NIC promiscuo legge tutti i pacchetti in transito
- può leggere tutti i dati criptati (p.es. password)
- e.g.: C "sniffa" i pacchetti di B



Minacce alla sicurezza di Internet

IP Spoofing:

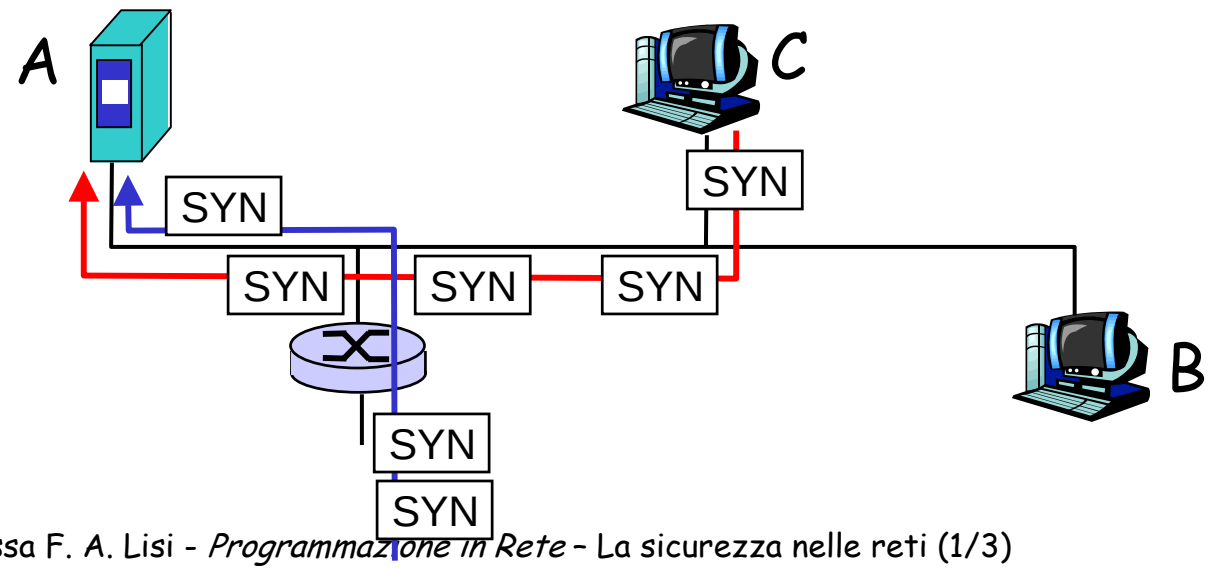
- può generare pacchetti "grezzi" IP direttamente dall'applicazione, inserendo un qualsiasi valore nel campo indirizzo IP sorgente
- il ricevente non sa se la sorgente è truffata
- e.g.: C fa finta di essere B



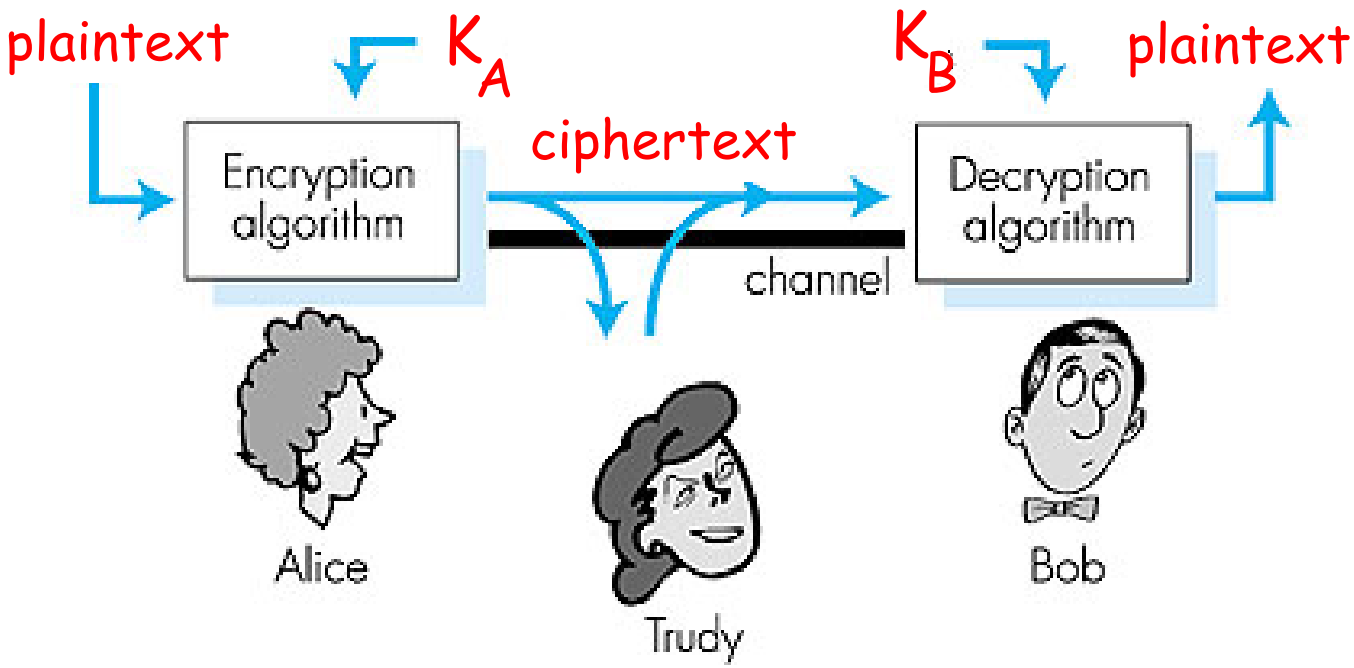
Minacce alla sicurezza di Internet

Denial of service (DOS):

- marea di pacchetti maliziosamente generati "inonda" il ricevente
- Distributed DOS (DDOS): sorgenti molteplici coordinate inondano il ricevente
- e.g., C ed un host remoto *SYN-attack* A



Il linguaggio della crittografia



Crittografia a chiave simmetrica: mittente e ricevente hanno chiavi identiche

crittografia a chiave pubblica: cifratura a chiave pubblica, decifratura a chiave *segreta*

Crittografia a chiave simmetrica

Cifra di sostituzione: sostituire una cosa per un'altra

- cifra monoalfabetica: sostituisci una lettera per un'altra

Testo in chiaro: abcdefghijklmnopqrstuvwxyz

Testo cifrato: mnbvcxzasdfghjklpoiuytrewq

E.g.: **In chiaro: bob. i love you. alice**

cifrato: nkn. s gktc wky. mgsbc

D: Quanto è difficile infrangere questo semplice codice?:

- brute force
- altro?

Crittografia a chiave simmetrica: DES (Data Encryption Standard)

- US encryption standard [NIST 1993]
- chiave simmetrica a 56 bit, input di testo in chiaro a 64 bit
- Quanto è sicuro?
  - DES Challenge: frase cifrata con chiave a 56 bit ("Strong cryptography makes the world a safer place") decifrata (brute force) in 4 mesi
  - nessun approccio noto di decodica "backdoor"
- rendere DES più sicuro
  - usare tre chiavi sequenzialmente (3-DES) su ogni dato
  - usare concatenamento dei blocchi cifrati

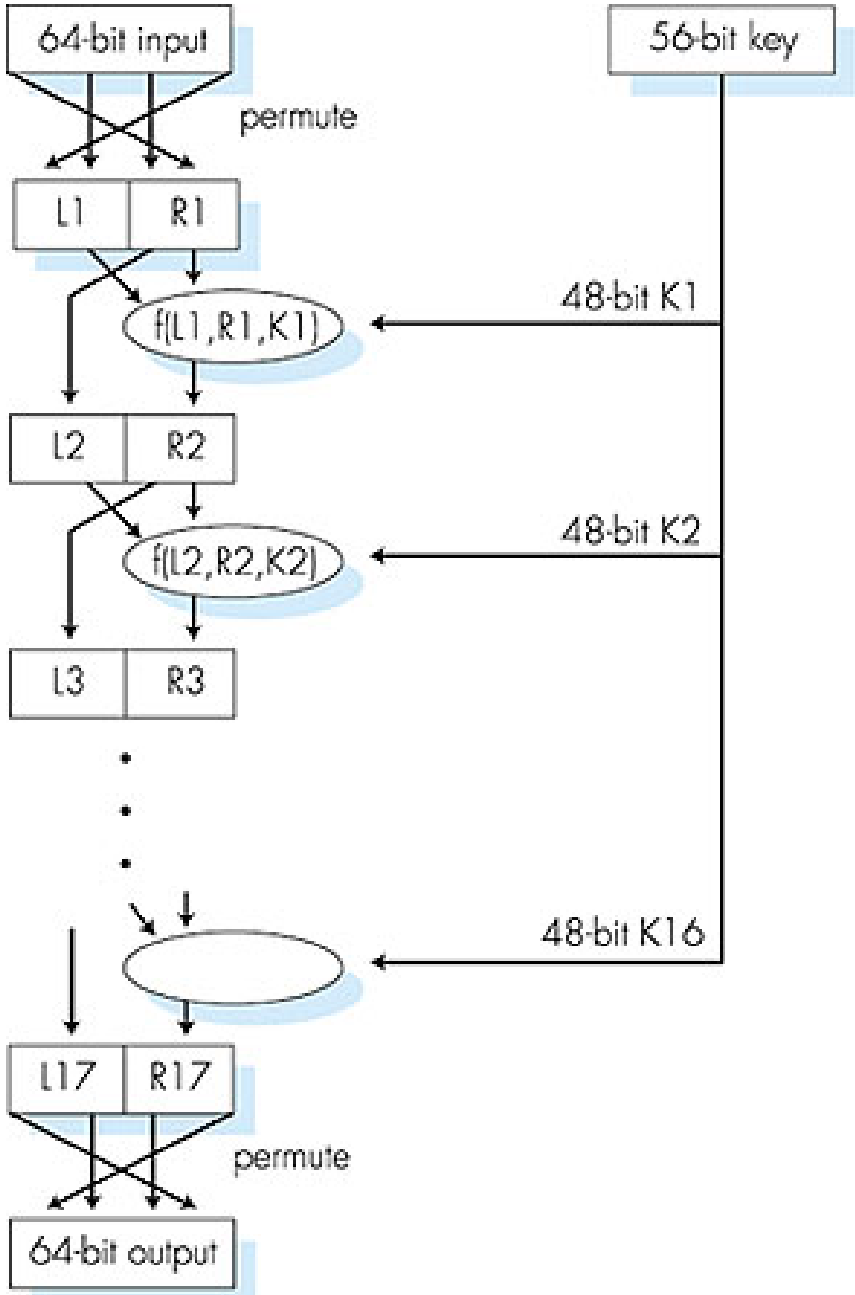
Crittografia a chiave simmetrica: DES

DES operation

Permutazione iniziale

16 cicli identici di applicazione di funzione, ciascuno dei quali usa 48 bit diversi della chiave

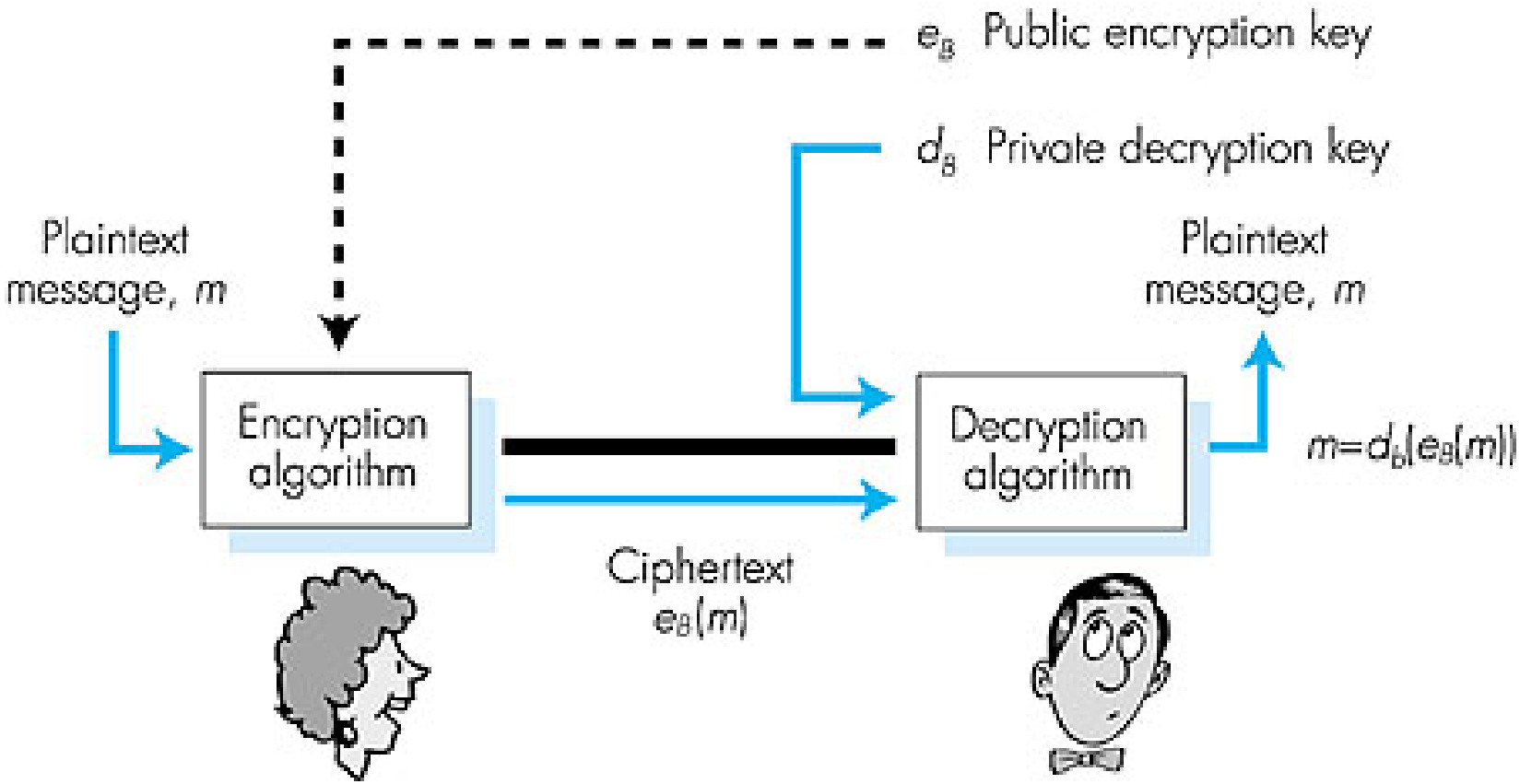
permutazione finale



Crittografia a chiave pubblica

- approccio radicalmente diverso dalla crittografia a chiave simmetrica [Diffie-Hellman76, RSA78]
- mittente e ricevente non condividono la chiave segreta
- la chiave di cifratura è *pubblica* (nota a *tutti)*
- la chiave di decifratura è privata (nota solo al ricevente)

Crittografia a chiave pubblica



Crittografia a chiave pubblica

Due requisiti interrelati:

1. need $d_B(\cdot)$ and $e_B(\cdot)$ such that
   $d_B(e_B(m)) = m$

2. need public and private keys for $d_B(\cdot)$ and $e_B(\cdot)$

RSA: Rivest, Shamir, Adelson algorithm

Crittografia a chiave pubblica: scelta delle chiavi in RSA

1. Scegliere due grandi numeri primi *p, q.* (e.g., ciascuno di 1024 bit)

2. Calcolare $n = pq$, $z = (p-1)(q-1)$

3. Scegliere e *(con* $e<n$*)* che non abbia fattori comuni con z. (*e, z* sono "relativamente primi").

4. Scegliere d tale che $ed-1$ sia esattamente divisibile per z. (in altri termini: $ed \bmod z = 1$).

5. La chiave *pubblica* è (n,e). La chiave *privata* è (n,d).

Crittografia a chiave pubblica: cifratura e decifratura in RSA

0. Dati (n,e) e (n,d) calcolati come visto prima

1. Per codificare il pattern di bit, m, calcola
   $c = m^e \bmod n$ (i.e., resto se m^e è diviso per n)

2. Per decifrare il pattern di bit ricevuto, c, calcola
   $m = c^d \bmod n$ (i.e., resto se c^d è diviso per n)

Magia!

$$m = (m^e \bmod n)^d \bmod n$$

Crittografia a chiave pubblica: un esempio di RSA

Bob sceglie *p=5, q=7*. Quindi *n=35, z=24*.

e=5 (così *e, z* relativamente primi).
d=29 (così *ed-1* esattamente divisibile per z).

	letter	m	m^e	$c = m^e \bmod n$
encrypt:	l	12	1524832	17

	c	c^d	$m = c^d \bmod n$	letter
decrypt:	17	48196857210675091509141182522307200 0	12	l

Sommario della prossima lezione: La sicurezza nelle reti (2/3)

Dai fondamenti ...

- che cosa è la sicurezza?
- crittografia
- autenticazione
- integrità e non ripudiabilità del messaggio
- distribuzione delle chiavi e certificazione

... in pratica

- a livello di applicazione: e-mail sicura
- a livello di trasporto: commercio Internet, SSL, SET
- a livello di rete: sicurezza IP